PCMJ

Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

SMART ROOM SYSTEM WITH DUAL AUTHENTICATION

MUHAMMAD HAZMI HARUN
College of Computing, Informatics and Mathematics, Universiti Teknologi MARA,
2022738927@student.uitm.edu.my

NURUL NAJWA ABDUL RAHID @ ABDUL RASHID*
College of Computing, Informatics and Mathematics, Universiti Teknologi MARA,
najwa193@uitm.edu.my

Article Info

Received: 17th February 2024
Accepted:
Available Online:

Abstract

This project aims to create a Smart Room System with Dual Authentication, which includes face recognition as the first security layer and a password as the second. This system depends on cloud-based storage, which is Firebase to improve security in a variety of situations. At its center, a Raspberry Pi with a webcam performs face scanning and captures face. A numeric keypad for password entry after face verification, a solenoid sensor for door locking, an LED light that can be controlled remotely via a mobile application, a buzzer for detecting failed attempts, and a DHT11 sensor for humidity and temperature monitoring inside the smart room are all equipment of additional IoT hardware. The face recognition system relies on OpenCV for accurate face detection, capturing face only during system operation, whether a successful or unsuccessful attempt occurs. It uses the Histogram of Oriented Gradients (HOG) algorithm for face recognition, which results in lower power consumption and faster processing. Captured face are also stored in Firebase Storage for cloud access, while the Raspberry Pi sends a copy to the administrator via email with attempt details as a notification. In addition, a mobile application enables the administrator to monitor the door lock state either locked or unlocked, temperature, humidity, and LED light status either on or off, as well as change the LED light remotely. This project demonstrates the seamless combination of hardware and software in order to develop a Smart Room that improves security, savings on energy, and user simplicity.

Keywords: Firebase, Histogram of Oriented Gradients, Face Recognition, Dual Authentication

INTRODUCTION (HEADING 1)

The Internet of Things (IoT) is a network of connected devices that share data via cloud computing. Ranging from household items to industrial machines, IoT devices use sensors and software to improve productivity, enhance customer experience, and support better decision-

making. One example is a Smart Room System. It is a system in which objects embedded with detector technology work to exchange and transfer information through a wireless communication medium without human interaction with any other object (Jion & Ahmad, 2024).

Smart Room System is defined as a technologically enhanced environment equipped with interconnected devices and system that automate and optimize various functions, utilize IoT technology, improve comfort, security and energy efficiency.Smart Rooms is very helpful in saving electricity and building this model is very economical (Karumuri & Yarlagadda, 2020).

Dual authentication is a security measure that requires more than simply a username and password for access. Moreover, the security risk associated with relying solely on one authentication method, without considering dual-authentication approaches, became evident as it left the system susceptible to unauthorized access through eavesdropping or code interception (Balfaqih, 2024).

In conclusion, this project integrates the dual authentication as security mechanism in a Smart Room System. The system not just secure the premise, it also can reduce the time to investigate when someone tried to breach the premise. With this system, it can provide a new method to ensure the premise is free from security breach using advanced technology to create a multi-layer protection for physical security and real-time response.

Problem Statement

Smart Room System only implemented single authentication which is Alphanumeric passwords. Alphanumeric passwords, for instance, often lead to weak choices, and susceptibility to brute force and dictionary attacks (Charan Ayineni et al., 2024). For example, using alphanumeric passwords usually ends in weak picks and makes you at risk of dictionary and brute force assaults.

Unauthorized influence is understood as an impact on protected information in violation of established rights and (or) access rules, leading to leakage, distortion, forgery, destruction, blocking of access to information, as well as to the loss, destruction or malfunction of the information carrier (Eryshov & Ilina, 2022). Providing a log system to the smart room system also can helps police officers when an event of a security breach occurs. Moreover, Digital Evidence used in criminal investigation could help reveal the unlawful act committed by the perpetrators (Hadi Kusuma & Khairunnisa, 2022).

Project Objectives

a) To design a Smart Room System with Dual Authentication.

b) To develop a Smart Room System with Dual Authentication.

c) To evaluate the functionality of the system.

Project Scopes

The Smart Room System features two user types: administrators and staff. Administrators manage users, security logs, and have full access, while staff can control lights, curtains, and temperature. Both must pass face recognition and keypad authentication to enter. The system uses a Raspberry Pi 4 Model B for its superior performance, built-in OS, and machine learning capabilities. It integrates a webcam, LED, solenoid lock, battery, relay module, keypad, and temperature-humidity sensor. The Histogram of Oriented Gradients algorithm enables face recognition, with Thonny IDE for coding and Firebase for storing credentials and logs. WiFi or LAN ensures updates, while Telnet or SSH supports registration. A mobile app, developed using MIT App Inventor, allows remote monitoring and control. This project emphasizes dual authentication to enhance security and protect valuable assets.

Project Significance

The Smart Room System with Dual Authentication enhances security by preventing unauthorized access to high-value assets. It protects client, staff, and company privacy through advanced technology and cloud-based data access. Dual authentication adds a layer of protection against password breaches, while access logs aid legal cases and security analysis. Its cloud adaptability ensures future compatibility, reinforcing security and safeguarding assets.

LITERATURE REVIEW

Smart Room with IoT Integration

Accordingly, a regular enhancement of related technologies is occurring as well, which in turn show a great influence on enterprise systems and information and communications technology (ICT) by means of improved connectivity, efficiency, scalability, time savings, and cost savings (Chowdhury & Raut, 2019). IoT architecture is the term used to describe the wide order of parts that made up IoT network system, consists of actuators, sensors, protocols, layer,

and cloud services (Nusrat et al., 2023). IoT integration is a process of connecting those IoT devices with physical object and data will be stored on cloud storage. These intelligent systems leverage sensors, actuators, and interconnected devices to create an environment that adapts to occupants' needs while prioritizing energy efficiency (Tiwari et al., 2024).

Raspberry Pi

The Raspberry Pi is a compact single-board computer with all essential components on one circuit board. It includes a GPU, CPU, USB ports, RAM, and an SD card slot, making it fully functional. Figure 1 shows the example of Raspberry Pi model 4 and its features.

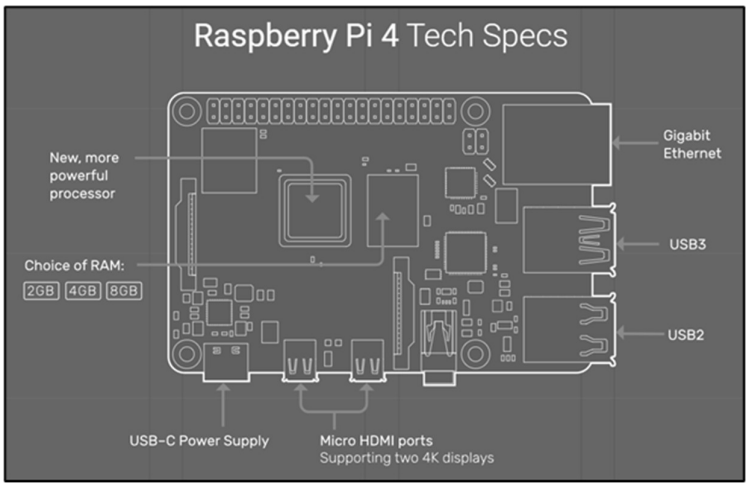

Figure 1: Raspberry Pi Model 4

Facial Recognition Biometric

Facial Recognition is a method for verifying the identity of a person using their face. Facial recognition systems can identify persons in pictures, videos, and in real time. Facial recognition works by comparing the faces of people passing by particular cameras to captures of persons on a watch list. (Alfattama et al., 2021) mentions that the problem of partial face recognition has become one of the increasing requirements in daily life applications such as surveillance camera systems for identification, whether in the home, robots, or computer vision systems inside mobile devices.

Histogram of Oriented Gradients

Histogram of Oriented Gradients (HOG) algorithm is a feature-based technique for face recognition that detects and describes faces by examining gradients from a picture. A system

is designed for extracting necessary features which plays important role in expression recognition of face (Maraskolhe & Bhalchandra, 2019). It separates the picture into small sections (cells), calculates the gradient direction and magnitude for each pixel, and then generates histograms summarizing the most frequent gradient directions in each cell. These histograms combine to generate a feature descriptor that captures the primary structural patterns of the face.

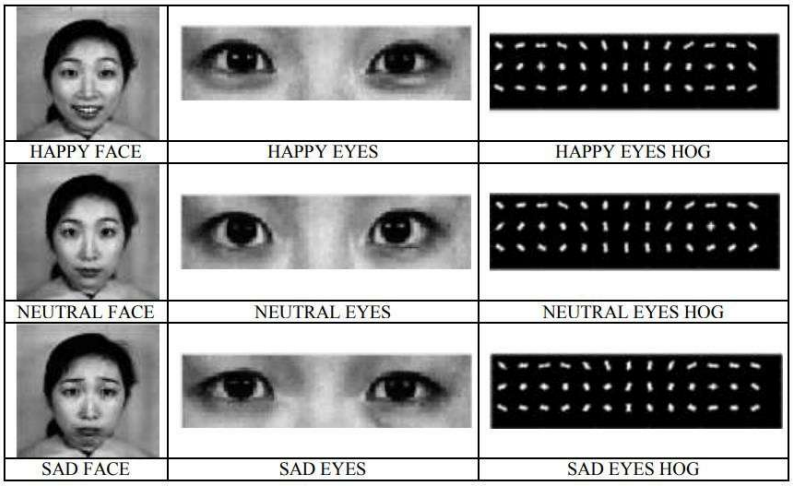

Figure 2: Histogram of Oriented Gradients Algorithm

Numeric Keypad as Authentication

Refers to (Shen et al., 2020) inputting the password using numerical keypad of smartphone is an essential step of the mobile payment process, which is prone to be attacked by malicious users.

Hybrid Cloud Storage

(Gorantla et al., 2024) says that hybrid cloud deployments extend the security, flexibility, scalability, and cost-effectiveness of traditional cloud computing architectures, as well as makes use of the latest cloud security protocols to ensure data is kept safe. Moreover, (Chermprayong & Kraichan, 2020) mentions that the advantage of the Hybrid Cloud is that it is suitable for enterprises that may want to combine public clouds, private clouds, and on-premises resources to gain competitive advantages of them all.

PROJECT METHODOLOGY

Project methodology is a structured approach to gathering, organizing, and executing projects. This project follows the adopted Waterfall model, which consists of six phases: Gathering Information (collecting data), Analysis (identifying hardware and software), Design (creating system architecture), Development (choosing programming languages), Testing (evaluating functionality), and Documentation (compiling all project details). Figure 3 and Table 1 outline each phase and its activities.

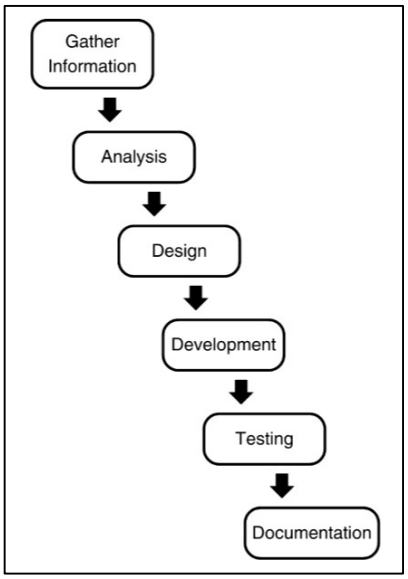

Figure 3: Adopted Waterfall Model

Gather Information

The project follows several phases: Analysis, summarizing the Literature Review (Chapter 2); Design, covering methodology tasks from weeks 10–12; Development, spanning semester 6 weeks 1–10, including system, database, application, and hardware integration; Testing, conducted weekly to ensure progress, involving software installation (OpenCV, Firebase, Thonny), hardware integration, and database connection; and Documentation, compiling all materials upon project completion.

Circuit Design

The Smart Room System with Dual Authentication uses a Raspberry Pi 4 B, connected to a keypad, buzzer, relay, solenoid lock, LED, DHT11 sensor, and webcam for face scanning. The DHT11 sends temperature and humidity data to Firebase via WiFi. A power adapter powers the Raspberry Pi, while 3x18650 batteries power the solenoid. The system updates

status via HTTP, sends email alerts, and allows mobile app control of room conditions. Firebase stores user data, sensor readings, and credentials.

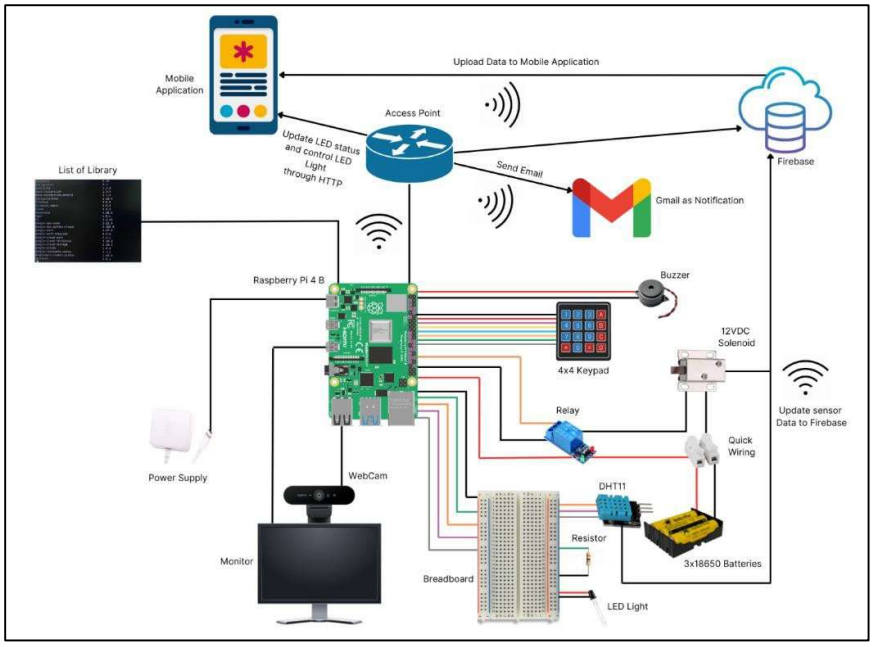

Figure 4: Circuit Design

Use Case Diagram

Figure 5 illustrates user and admin interaction with the Smart Door System. Users must pass face scanning and password entry to unlock the door for five seconds. After three failed attempts, the system captures their image, logs it in the database, and alerts the admin via email. Admins manage user registration, access logs, and security settings remotely via Putty. They can monitor and control LED status, temperature, humidity, and door locks through a mobile app. Only admins can register users, ensuring system security and preventing unauthorized access.

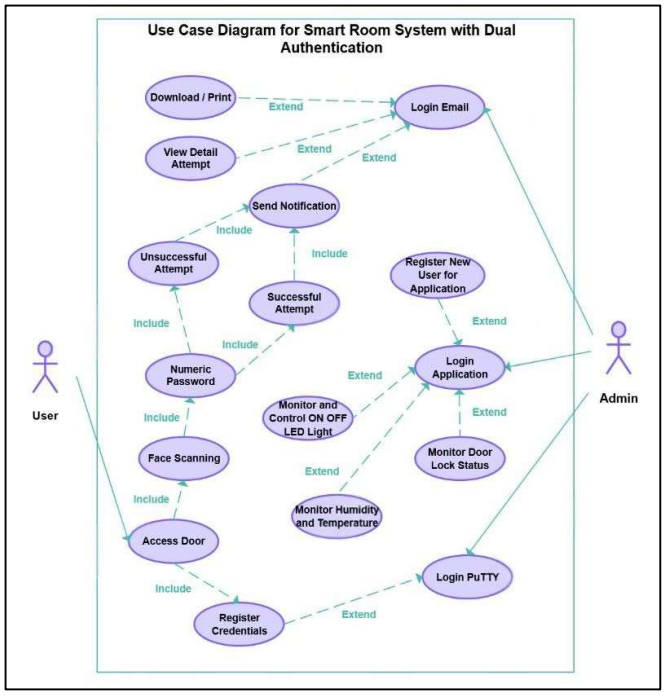

Figure 5: Use Case Diagram for Smart Room System with Dual Authentication

Flowchart

Flowchart is used for helps readers to understand complex ideas by illustrating the logical flow of system activities. According to (Leena & Ganesh, 2020) flowchart as infographics is a simple but effective way to represent a sequence of operations to be performed using symbols and text. It is also illustrating the operation of the system, item interactions, and decision-making processes.

Figure 6 illustrates the door access flowchart. The process starts when a user presses “A” to initiate face recognition. If recognized, the system displays the staff ID and prompts for a password. Users have three attempts before the system logs the attempt, notifies the admin via email, and restarts. If the password is correct, the door unlocks for five seconds before relocking.

PCMJ
Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

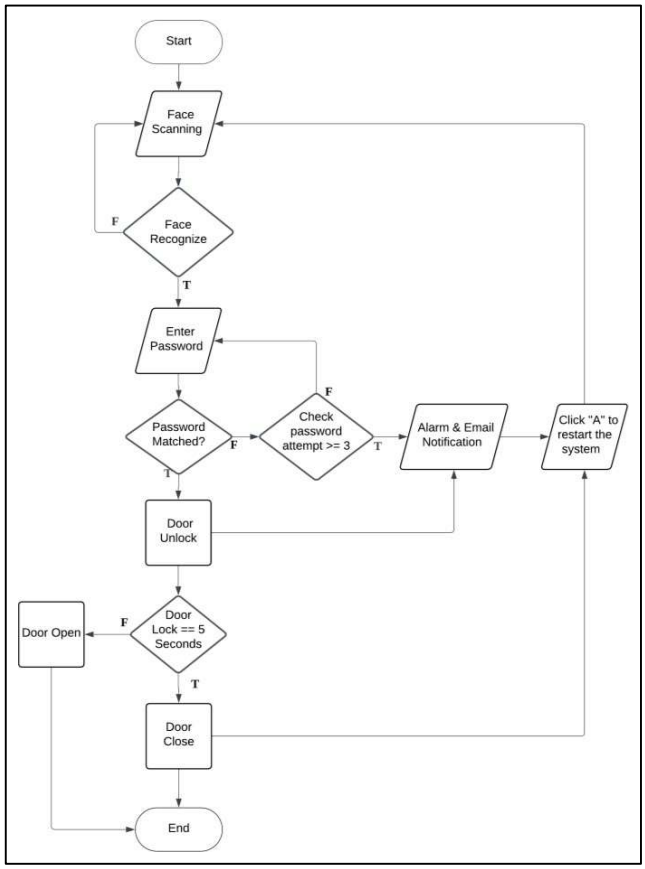

Figure 6: Flowchart for Door Access

RESULT AND DISCUSSION

The system is developed in Python using the Histogram of Oriented Gradients (HOG) algorithm for face recognition. OpenCV captures images from the webcam, encodes faces into numerical data, and stores them in Firebase Firestore. The HOG algorithm converts images to greyscale, divides them into 8x8 cells, groups them into 2x2 blocks for contrast adjustment, and creates a gradient-based feature vector for recognition. (Maraskolhe & Bhalchandra, 2019) mentions that Magnitude and orientation at each picture element I(x,y) is calculated by,

Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

$$\mu = Gmag(x,y) = \sqrt{Gx^2(x,y) + Gy^2(x,y)}$$

$$\theta(x,y) = \arctan\left(\frac{Gy(x,y)}{Gx(x,y)}\right) + \pi/2$$

Figure 7: Formula of Histogram of Oriented Gradients Algorithm

Hardware Setup

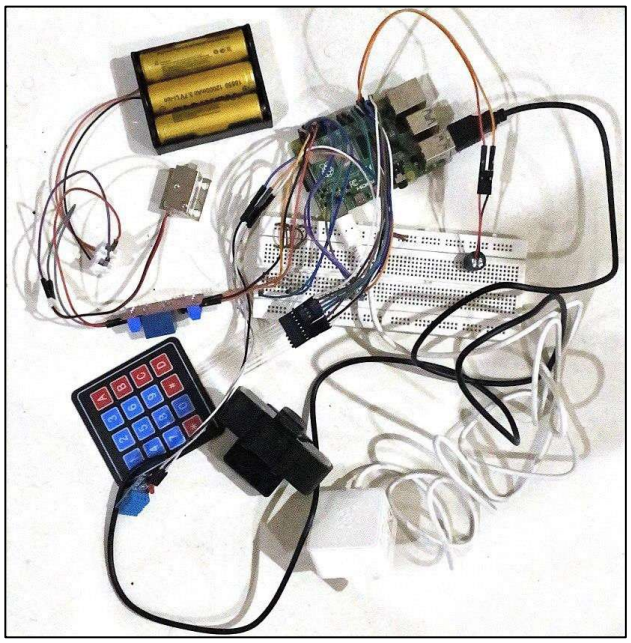

Figure 8: Hardware Setup

The Raspberry Pi connects to a webcam via USB for face recognition and user record-keeping in an online database. A 4x4 keypad, linked to GPIOs 6, 13, 19, and 26 (rows) and 5, 11, 9, and 21 (columns), handles second-stage authentication. A buzzer on GPIO 16 alerts failed attempts. The 12VDC solenoid door lock, controlled by a 1-channel relay module, connects to GPIO 17, GND, and 5V PWR, powered by 3x18650 batteries through a CH-2 Quick Wiring Terminal. A breadboard links the DHT11 sensor (GPIO 23) for temperature and humidity monitoring and an LED (GPIO 18) for remote control via the application.

Face Recognition for Smart Door System

After user enter correct password, the system will unlock the door for 5 seconds. The door lock status will be uploaded to the Firebase and mobile application. System will not forget to capture the user face even the user is authorized to the Smart Room for log use in Firebase Storage.

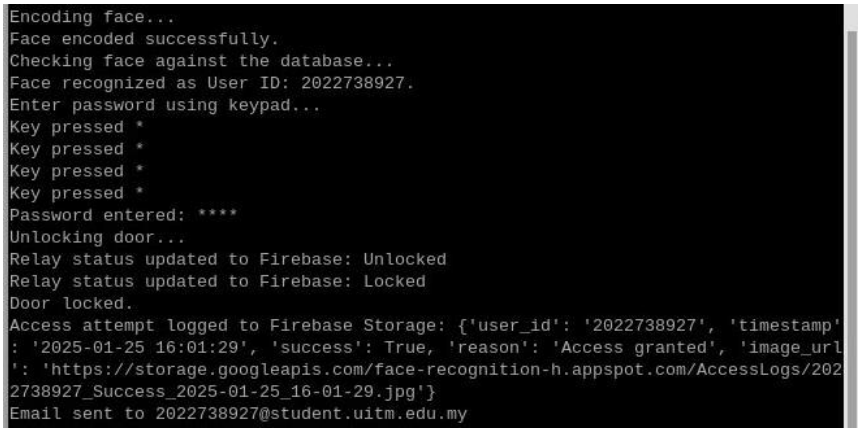

Figure 9: Result of Success Attempt

Every login attempt, whether successful or failed, is recorded in Firebase and emailed to the administrator. The email's "Reason" section indicates if access was granted (correct password), denied (exceeded attempts), or marked as unknown (unrecognized face or no detection).

Figure 10: Result of Success Granted in Email

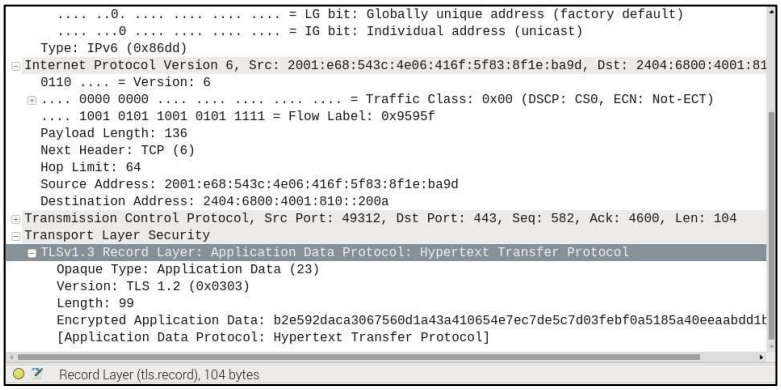

Figure 11: Detail Packet from Raspberry Pi to Firebase

Figure 11 show that Raspberry Pi communicates with Firebase using TLSv1.3 for secure data transmission. TLSv1.3 enhances speed and security by using dynamic session keys, preventing attackers from decrypting messages, including hashed user passwords. Encryption and decryption occur during the TLS handshake between the client and server.

CONCLUSION

This chapter concludes the project, discussing its achievements, limitations, and future improvements. The Smart Door System with Dual Authentication, using Raspberry Pi 4B and a mobile app, successfully integrates face recognition and password authentication with Firebase to enhance security. The system ensures only registered users gain access, while access history tracking logs all login attempts and alerts the administrator in real time. Its user-friendly app allows monitoring and control of LED lights, door locks, temperature, and humidity. However, the system relies on a stable internet connection for authentication, affecting performance in low-connectivity areas. Future enhancements could include advanced network security features like a Kibana Dashboard for detailed monitoring and analytics.

Project Limitation

The system's reliance on an internet connection was a major limitation, as Firebase handled user credential matching and data storage. Slow internet caused delays in face scanning, password verification, and data logging. Network tests showed that lower speeds significantly increased authentication time. Additionally, the application could be improved to give administrators more control, such as tracking user entries, incorrect password attempts,

and failed face scans. A more advanced dashboard like Kibana could enhance security, but Firebase and MIT App Inventor impose server restrictions, requiring Firebase to be set to a US server for full compatibility.

Recommendation

Future improvements could include adding biometric authentication like iris scanning and fingerprint recognition to strengthen security and reduce false positives. Implementing liveness detection would also prevent spoofing attempts using photos or videos. Additionally, integrating advanced analytics dashboards like Kibana or Grafana into the mobile app could provide real-time visualizations of user access trends, failed attempts, and security alerts. These features would help administrators monitor patterns, detect vulnerabilities, and receive instant alerts for suspicious activity, enhancing response times and overall security.

REFERENCES

Alfattama, S., Kanungo, P., & Bisoy, S. K. (2021). Face Recognition from Partial Face Data. 2021 International Conference in Advances in Power, Signal, and Information Technology, APSIT 2021. https://doi.org/10.1109/APSIT52773.2021.9641286

Balfaqih, M. (2024). Enhancing Security and Flexibility in Smart Locker Systems: A Multi-Authentication Approach with IoT Integration. 21st International Learning and Technology Conference: Reality and Science Fiction in Education, L and T 2024, 325–329. https://doi.org/10.1109/LT60077.2024.10469610

Charan Ayineni, K. S., Pranav, P. M. V., & Vasanth, A. V. (2024). Enhancing Authentication Security: Emoji based Graphical Passwords in Universal Three-Factor Authentication Systems. 7th International Conference on Inventive Computation Technologies, ICICT 2024, 2152–2159. https://doi.org/10.1109/ICICT60155.2024.10544476

Chermprayong, P., & Kraichan, C. (2020). 3D Scanning with AI-powered Embedded System Streaming Digital Signage via Redundant Network Attached Storage and Hybrid Cloud Storage.

Chowdhury, A., & Raut, S. A. (2019). Benefits, challenges, and opportunities in adoption of Industrial IoT.

Eryshov, V. G., & Ilina, D. V. (2022). Markov Model of the Computer Intelligence Process that Provides Unauthorized Access and Obtaining Confidential Information from Information Systems of Organizations. Wave Electronics and Its Application in Information and Telecommunication Systems, WECONF - Conference Proceedings. https://doi.org/10.1109/WECONF55058.2022.9803467

Gorantla, V. A. K., Gude, V., Sriramulugari, S. K., Yuvaraj, N., & Yadav, P. (2024). Utilizing Hybrid Cloud Strategies to Enhance Data Storage and Security in E-Commerce Applications. 2024 2nd International Conference on Disruptive Technologies, ICDT 2024, 494–499. https://doi.org/10.1109/ICDT61202.2024.10489749

Hadi Kusuma, M. J., & Khairunnisa, R. (2022). Forensic Imaging Integrity Guarantor using Raspberry Pi and RFID Tag. ICOSNIKOM 2022 - 2022 IEEE International Conference of Computer Science and Information Technology: Boundary Free: Preparing Indonesia for Metaverse Society. https://doi.org/10.1109/ICOSNIKOM56551.2022.10034877

Jion, Md. S. A., & Ahmad, M. (2024). A Smart and Secured Office System Using IoT. 2024 International Conference on Advances in Computing, Communication, Electrical, and Smart Systems (ICACCESS), 1–6. https://doi.org/10.1109/iCACCESS61735.2024.10499529

Karumuri, L. S., & Yarlagadda, A. (2020, December 10). Smart Rooms. 2020 IEEE 17th India Council International Conference, INDICON 2020. https://doi.org/10.1109/INDICON49873.2020.9342283

Leena, C., & Ganesh, M. (2020, February 1). Generating Graph from 2D Flowchart using Region-Based Segmentation. 2020 IEEE International Students' Conference on Electrical, Electronics and Computer Science, SCEECS 2020. https://doi.org/10.1109/SCEECS48394.2020.165

Maraskolhe, P. N., & Bhalchandra, A. S. (2019). Analysis of Facial Expression Recognition using Histogram of Oriented Gradient (HOG). IEEE.

Nusrat, M. A., Paul, S., & Bhushan, B. (2023). Practicle Coordination and Aspect of IoT for Smart Cities and Healthcare System. Proceedings of the 2023 12th International Conference on System Modeling and Advancement in Research Trends, SMART 2023, 280–287. https://doi.org/10.1109/SMART59791.2023.10428643

Shen, X., Yan, G., Yang, J., & Xu, S. (2020). WiPass: CSI-based keystroke recognition for numerical keypad of smartphones. Proceedings - 2020 35th Youth Academic Annual Conference of Chinese Association of Automation, YAC 2020, 276–283. https://doi.org/10.1109/YAC51587.2020.9337673

Tiwari, S., Bhushan, A., Singh, A. K., & Yadav, R. K. (2024). Unleashing the Potential of IoT Integration for Energy Optimization in Smart Homes. 82–85. https://doi.org/10.1109/parc59193.2024.10486624